JCATTファイルフォーマット仕様書

CCMモード

２００８年4月１１日

独立行政法人　情報処理推進機構

目 次

1　はじめに

暗号アルゴリズム実装試験ツール (以下 JCATT と略記する) が使用する各種ファイルのフォーマット規則を記述する．JCATT が使用するファイルには次のようなものがある．

ファイルの種類

- パラメータファイル (*.par)
  試験項目の設定を記述する．JCATT を用いて作成する．
- リクエストファイル (*.req)
  暗号モジュール開発ベンダに対する要求を記述する．JCATT を用いて作成する．
- Facts ファイル (*.fax)
  テストベクタを記述する．JCATT を用いて作成する．
- レスポンスファイル (*.rsp)
  ベンダからの回答を記述する．リクエストファイルおよび本稿で指定するファイルフォーマットに基づいてベンダが作成する．
- 結果ファイル (*.out)
  試験結果を記述する．JCATT を用いて作成する．

これらのファイルの名前は，次の規則に従ってつけること．

ファイル名の規則

- 拡張子は，上記 ( ) 内に指定したものを使用すること．
- 拡張子以外の名前は，試験対象暗号モジュールごとに同じ名称をつけること．
  リクエストファイル (*.req) と Facts ファイル (*.fax) の生成時には，リクエストファイル (*.req) と Facts ファイル (*.fax) に対してパラメータファイル (*.par) と同じ名称を JCATT が自動的につける．
  試験実行時には，同じ名称のレスポンスファイル (*.rsp) と Facts ファイル (*.fax) に対して試験が行われる．また，試験実行時は，結果ファイル (*.out) に対して，Facts ファイル (*.fax) と同じ名称を JCATT が自動的につける．

ファイルフォーマット詳細は次章以降に記述する．各ファイルに共通の規則は次の通りである．

共通規則

- [　] で囲まれた “タグ” の次の行に値を記述する．
- タグは各ファイルフォーマットに記述した順番通りに記述すること．
- レスポンスファイルにおいては,【出力】と記述したタグが，試験対象モジュールが出力するデータを記述する箇所である．
- 半角英数字を用いること．
- タグおよび値は大文字小文字の区別をするので，大文字小文字を含めて正確に記述すること．ただし，数値を 16 進数で記述する場合は，大文字小文字は区別しない．
- 一文字目が ♯(半角) で始まるコメント行を自由に書き込むことができる．
- 平文，暗号文，鍵などのデータの区切り文字は改行 (CR+LF または LF) とする．
- 平文，暗号文，署名，鍵などのデータは 16 進表記とする．
- ビット数，個数などの数値は 10 進表記とする．
- ACSII コードを使用すること．
- 各行には必ず改行を入れること (最後のデータと EOF との間にも改行を入れること)．

2 CCM モード

CCM（Counter with Cipher Block Chaining-Message Authentication Code）モードの暗号アルゴリズム実装試験のためのファイルフォーマットを記述する．

各表において，試験方法に関する以下の略語を使用する．

- VADT: 種々の associated data に対する試験 (The Variable Associated Data Test)
- VPT: 種々の平文に対する試験 (The Variable Payload Test)
- VNT: 種々の nonce に対する試験 (The Variable Nonce Test)
- VTT: 種々のメッセージ認証子に対する試験 (The Variable Tag Test)

試験方法の詳細は，暗号アルゴリズム実装試験仕様書を参照のこと．

各表におけるブロック暗号の識別子は次表の通り．

表 1: ブロック暗号識別子

ブロック暗号識別子	対応するブロック暗号
M_BlockCipher_AES	AES
M_BlockCipher_CAMELLIA	Camellia
M_BlockCipher_CIPHERUNICORN_A	CIPHERUNICORN-A
M_BlockCipher_HIEROCRYPT_3	Hierocrypt-3
M_BlockCipher_SC2000	SC2000

2.1 パラメータファイル (*.par)

表 2: CCM モードパラメータファイル

機能	タグ	内容
(共通)	[Algorithm Name]	CCM
暗号化	[Function Name]	Encryption
	[Block Cipher]	CCM 内部で使用するブロック暗号識別子
	[Bitlength of Key]	鍵のビット長，128 または 192 または 256
	[Seed]	ランダムデータを生成するための擬似乱数生成関数用シード値
	[Bitlength of Seed]	Seed のビット長
	[Number of Payloads for VADT]	VADT 用平文の個数
	[Key for VADT]	VADT 用鍵
	[Bitlength of Nonce for VADT]	VADT 用 nonce のビット長
	[Nonce for VADT]	VADT 用 nonce
	[Bitlength of Associated data for VADT]	VADT 用 associated data のビット長
	[Number of Payloads for VPT]	VPT 用平文の個数
	[Key for VPT]	VPT 用鍵
	[Bitlength of Nonce for VPT]	VPT 用 nonce のビット長
	[Nonce for VPT]	VPT 用 nonce
	[Bitlength of Payload for VPT]	VPT 用平文のビット長
	[Number of Payloads for VNT]	VNT 用平文の個数
	[Key for VNT]	VNT 用鍵
	[Bitlength of Nonce for VNT]	VNT 用 nonce のビット長
	[Number of Payloads for VTT]	VTT 用平文の個数
	[Bitlength of Tag for VTT]	VTT 用メッセージ認証子のビット長
	[Key for VTT]	VTT 用鍵
	[Bitlength of Nonce for VTT]	VTT 用 nonce のビット長
	[Nonce for VTT]	VTT 用 nonce

表 3: CCM モードパラメータファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	CCM
復号	[Function Name]	Decryption
	[Block Cipher]	CCM 内部で使用するブロック暗号識別子
	[Bitlength of Key]	鍵のビット長，128 または 192 または 256
	[Seed]	ランダムデータを生成するための擬似乱数生成関数用シード値
	[Bitlength of Seed]	Seed のビット長
	[Number of Ciphertexts]	暗号文の個数
	[Bitlength of Tag]	メッセージ認証子のビット長
	[Bitlength of Payload]	平文のビット長
	[Rate of Fail Data]	復号失敗用データの割合

2.2 リクエストファイル (*.req)

表 4: CCM モードリクエストファイル

機能	タグ	内容
(共通)	[Algorithm Name]	CCM
暗号化	[Function Name]	Encryption
	[Block Cipher]	CCM 内部で使用するブロック暗号識別子
	[Bitlength of Key]	鍵のビット長，128 または 192 または 256 [10 進数表記]
	[Number of Payloads for VADT]	VADT 用平文の個数 [10 進数表記]
	[Bitlength of Tag for VADT]	VADT 用メッセージ認証子のビット長 [10 進数表記]
	[Key for VADT]	VADT 用鍵 [16 進数表記]
	[Bitlength of Nonce for VADT]	VADT 用 nonce のビット長 [10 進数表記]
	[Nonce for VADT]	VADT 用 nonce [16 進数表記]
	[Bitlength of Associated data for VADT]	VADT 用 associated data のビット長 [10 進数表記]
	[Associated datas for VADT][1]	VADT 用 associated data [16 進数表記]
	[Bitlength of Payload for VADT]	VADT 用平文のビット長 [10 進数表記]
	[Payloads for VADT][1]	VADT 用平文 [16 進数表記]
	[Number of Payloads for VPT]	VPT 用平文の個数 [10 進数表記]
	[Bitlength of Tag for VPT]	VPT 用メッセージ認証子のビット長 [10 進数表記]
	[Key for VPT]	VPT 用鍵 [16 進数表記]
	[Bitlength of Nonce for VPT]	VPT 用 nonce のビット長 [10 進数表記]
	[Nonce for VPT]	VPT 用 nonce [16 進数表記]
	[Bitlength of Associated data for VPT]	VPT 用 associated data のビット長 [10 進数表記]
	[Associated datas for VPT][2]	VPT 用 associated data [16 進数表記]
	[Bitlength of Payload for VPT]	VPT 用平文のビット長 [10 進数表記]
	[Payloads for VPT][2]	VPT 用平文 [16 進数表記]
	[Number of Payloads for VNT]	VNT 用平文の個数 [10 進数表記]
	[Bitlength of Tag for VNT]	VNT 用メッセージ認証子のビット長 [10 進数表記]
	[Key for VNT]	VNT 用鍵 [16 進数表記]
	[Bitlength of Nonce for VNT]	VNT 用 nonce のビット長 [10 進数表記]
	[Nonces for VNT][3]	VNT 用 nonce [16 進数表記]
	[Bitlength of Associated data for VNT]	VNT 用 associated data のビット長 [10 進数表記]
	[Associated datas for VNT][3]	VNT 用 associated data [16 進数表記]
	[Bitlength of Payload for VNT]	VNT 用平文のビット長 [10 進数表記]
	[Payloads for VNT][3]	VNT 用平文 [16 進数表記]
	[Number of Payloads for VTT]	VTT 用平文の個数 [10 進数表記]
	[Bitlength of Tag for VTT]	VTT 用メッセージ認証子のビット長 [10 進数表記]
	[Key for VTT]	VTT 用鍵 [16 進数表記]
	[Bitlength of Nonce for VTT]	VTT 用 nonce のビット長 [10 進数表記]
	[Nonce for VTT]	VTT 用 nonce [16 進数表記]
	[Bitlength of Associated data for VTT]	VTT 用 associated data のビット長 [10 進数表記]
	[Associated datas for VTT][4]	VTT 用 associated data [16 進数表記]
	[Bitlength of Payload for VTT]	VTT 用平文のビット長 [10 進数表記]
	[Payloads for VTT][4]	VTT 用平文 [16 進数表記]

注

1. [Number of Payloads for VADT] 個のデータを記述する.
2. [Number of Payloads for VPT] 個のデータを記述する.
3. [Number of Payloads for VNT] 個のデータを記述する.
4. [Number of Payloads for VTT] 個のデータを記述する.

表 5: CCM モードリクエストファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	CCM
復号	[Function Name]	Decryption
	[Block Cipher]	CCM 内部で使用するブロック暗号識別子
	[Bitlength of Key]	鍵のビット長，128 または 192 または 256 [10 進数表記]
	[Number of Ciphertexts]	暗号文の個数 [10 進数表記]
	[Bitlength of Tag]	メッセージ認証子のビット長 [10 進数表記]
	[Bitlength of Payload]	平文のビット長 [10 進数表記]
	[Keys][1]	鍵 [16 進数表記]
	[Bitlength of Nonce]	nonce のビット長 [10 進数表記]
	[Nonces][1]	nonce [16 進数表記]
	[Bitlength of Associated data]	associated data のビット長 [10 進数表記]
	[Associated datas][1]	associated data [16 進数表記]
	[Ciphertexts][1]	暗号文 [16 進数表記]

注

1. [Number of Ciphertexts] 個のデータを記述する.

2.3 Facts ファイル (*.fax)

表 6: CCM モード Facts ファイル

機能	タグ	内容
(共通)	[Algorithm Name]	CCM
暗号化	[Function Name]	Encryption
	[Block Cipher]	CCM 内部で使用するブロック暗号識別子
	[Bitlength of Key]	鍵のビット長，128 または 192 または 256
	[Number of Payloads for VADT]	VADT 用平文の個数
	[Bitlength of Tag for VADT]	VADT 用メッセージ認証子のビット長
	[Key for VADT]	VADT 用鍵
	[Bitlength of Nonce for VADT]	VADT 用 nonce のビット長
	[Nonce for VADT]	VADT 用 nonce
	[Bitlength of Associated data for VADT]	VADT 用 associated data のビット長
	[Associated datas for VADT][1]	VADT 用 associated data
	[Bitlength of Payload for VADT]	VADT 用平文のビット長
	[Payloads for VADT][1]	VADT 用平文
	[Ciphertexts for VADT][1]	VADT 用期待値暗号文
	[Number of Payloads for VPT]	VPT 用平文の個数
	[Bitlength of Tag for VPT]	VPT 用メッセージ認証子のビット長
	[Key for VPT]	VPT 用鍵
	[Bitlength of Nonce for VPT]	VPT 用 nonce のビット長
	[Nonce for VPT]	VPT 用 nonce
	[Bitlength of Associated data for VPT]	VPT 用 associated data のビット長
	[Associated datas for VPT][2]	VPT 用 associated data
	[Bitlength of Payload for VPT]	VPT 用平文のビット長
	[Payloads for VPT][2]	VPT 用平文
	[Ciphertexts for VPT][2]	VPT 用期待値暗号文
	[Number of Payloads for VNT]	VNT 用平文の個数
	[Bitlength of Tag for VNT]	VNT 用メッセージ認証子のビット長
	[Key for VNT]	VNT 用鍵
	[Bitlength of Nonce for VNT]	VNT 用 nonce のビット長
	[Nonces for VNT][3]	VNT 用 nonce
	[Bitlength of Associated data for VNT]	VNT 用 associated data のビット長
	[Associated datas for VNT][3]	VNT 用 associated data
	[Bitlength of Payload for VNT]	VNT 用平文のビット長
	[Payloads for VNT][3]	VNT 用平文
	[Ciphertexts for VNT][3]	VNT 用期待値暗号文
	[Number of Payloads for VTT]	VTT 用平文の個数
	[Bitlength of Tag for VTT]	VTT 用メッセージ認証子のビット長
	[Key for VTT]	VTT 用鍵
	[Bitlength of Nonce for VTT]	VTT 用 nonce のビット長
	[Nonce for VTT]	VTT 用 nonce
	[Bitlength of Associated data for VTT]	VTT 用 associated data のビット長
	[Associated datas for VTT][4]	VTT 用 associated data
	[Bitlength of Payload for VTT]	VTT 用平文のビット長
	[Payloads for VTT][4]	VTT 用平文
	[Ciphertexts for VTT][4]	VTT 用期待値暗号文

注

1. [Number of Payloads for VADT] 個のデータを記述する.
2. [Number of Payloads for VPT] 個のデータを記述する.
3. [Number of Payloads for VNT] 個のデータを記述する.
4. [Number of Payloads for VTT] 個のデータを記述する.

表 7: CCM モード Facts ファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	CCM
復号	[Function Name]	Decryption
	[Block Cipher]	CCM 内部で使用するブロック暗号識別子
	[Bitlength of Key]	鍵のビット長，128 または 192 または 256
	[Number of Ciphertexts]	暗号文の個数
	[Bitlength of Tag]	メッセージ認証子のビット長
	[Bitlength of Payload]	平文のビット長
	[Keys][1]	鍵
	[Bitlength of Nonce]	nonce のビット長
	[Nonces][1]	nonce
	[Bitlength of Associated data]	associated data のビット長
	[Associated datas][1]	associated data
	[Ciphertexts][1]	暗号文
	[Payloads][2]	平文

注

1. [Number of Ciphertexts] 個のデータを記述する．
2. [Number of Ciphertexts] 個の平文を記述する．復号に失敗した場合は，[Payloads] データの該当行に INVALID と記述する．

2.4 レスポンスファイル (*.rsp)

表 8: CCM モードレスポンスファイル

機能	タグ	内容
(共通)	[Algorithm Name]	CCM
暗号化	[Function Name]	Encryption
	[Block Cipher]	CCM 内部で使用するブロック暗号識別子
	[Bitlength of Key]	鍵のビット長，128 または 192 または 256 [10 進数表記]
	[Number of Payloads for VADT]	VADT 用平文の個数 [10 進数表記]
	[Bitlength of Tag for VADT]	VADT 用メッセージ認証子のビット長 [10 進数表記]
	[Key for VADT]	VADT 用鍵 [16 進数表記]
	[Bitlength of Nonce for VADT]	VADT 用 nonce のビット長 [10 進数表記]
	[Nonce for VADT]	VADT 用 nonce [16 進数表記]
	[Bitlength of Associated data for VADT]	VADT 用 associated data のビット長 [10 進数表記]
	[Associated datas for VADT][1]	VADT 用 associated data [16 進数表記]
	[Bitlength of Payload for VADT]	VADT 用平文のビット長 [10 進数表記]
	[Payloads for VADT][1]	VADT 用平文 [16 進数表記]
	[Ciphertexts for VADT][1]	【出力】VADT で生成された暗号文 [16 進数表記]
	[Number of Payloads for VPT]	VPT 用平文の個数 [10 進数表記]
	[Bitlength of Tag for VPT]	VPT 用メッセージ認証子のビット長 [10 進数表記]
	[Key for VPT]	VPT 用鍵 [16 進数表記]
	[Bitlength of Nonce for VPT]	VPT 用 nonce のビット長 [10 進数表記]
	[Nonce for VPT]	VPT 用 nonce [16 進数表記]
	[Bitlength of Associated data for VPT]	VPT 用 associated data のビット長 [10 進数表記]
	[Associated datas for VPT][2]	VPT 用 associated data [16 進数表記]
	[Bitlength of Payload for VPT]	VPT 用平文のビット長 [10 進数表記]
	[Payloads for VPT][2]	VPT 用平文 [16 進数表記]
	[Ciphertexts for VPT][2]	【出力】VPT で生成された暗号文 [16 進数表記]
	[Number of Payloads for VNT]	VNT 用平文の個数 [10 進数表記]
	[Bitlength of Tag for VNT]	VNT 用メッセージ認証子のビット長 [10 進数表記]
	[Key for VNT]	VNT 用鍵 [16 進数表記]
	[Bitlength of Nonce for VNT]	VNT 用 nonce のビット長 [10 進数表記]
	[Nonces for VNT][3]	VNT 用 nonce [16 進数表記]
	[Bitlength of Associated data for VNT]	VNT 用 associated data のビット長 [10 進数表記]
	[Associated datas for VNT][3]	VNT 用 associated data [16 進数表記]
	[Bitlength of Payload for VNT]	VNT 用平文のビット長 [10 進数表記]
	[Payloads for VNT][3]	VNT 用平文 [16 進数表記]
	[Ciphertexts for VNT][3]	【出力】VNT で生成された暗号文 [16 進数表記]
	[Number of Payloads for VTT]	VTT 用平文の個数 [10 進数表記]
	[Bitlength of Tag for VTT]	VTT 用メッセージ認証子のビット長 [10 進数表記]
	[Key for VTT]	VTT 用鍵 [16 進数表記]
	[Bitlength of Nonce for VTT]	VTT 用 nonce のビット長 [10 進数表記]
	[Nonce for VTT]	VTT 用 nonce [16 進数表記]
	[Bitlength of Associated data for VTT]	VTT 用 associated data のビット長 [10 進数表記]
	[Associated datas for VTT][4]	VTT 用 associated data [16 進数表記]
	[Bitlength of Payload for VTT]	VTT 用平文のビット長 [10 進数表記]
	[Payloads for VTT][4]	VTT 用平文 [16 進数表記]
	[Ciphertexts for VTT][4]	【出力】VTT で生成された暗号文 [16 進数表記]

注

1. [Number of Payloads for VADT] 個のデータを記述する.
2. [Number of Payloads for VPT] 個のデータを記述する.
3. [Number of Payloads for VNT] 個のデータを記述する.
4. [Number of Payloads for VTT] 個のデータを記述する.

表 9: CCM モードレスポンスファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	CCM
復号	[Function Name]	Decryption
	[Block Cipher]	CCM 内部で使用するブロック暗号識別子
	[Bitlength of Key]	鍵のビット長，128 または 192 または 256 [10 進数表記]
	[Number of Ciphertexts]	暗号文の個数 [10 進数表記]
	[Bitlength of Tag]	メッセージ認証子のビット長 [10 進数表記]
	[Bitlength of Payload]	平文のビット長 [10 進数表記]
	[Keys][1]	鍵 [16 進数表記]
	[Bitlength of Nonce]	nonce のビット長 [10 進数表記]
	[Nonces][1]	nonce [16 進数表記]
	[Bitlength of Associated data]	associated data のビット長 [10 進数表記]
	[Associated datas][1]	associated data [16 進数表記]
	[Ciphertexts][1]	暗号文 [16 進数表記]
	[Payloads][2]	【出力】平文 [16 進数表記]

注

1. [Number of Ciphertexts] 個のデータを記述する．
2. [Number of Ciphertexts] 個の平文を記述する．復号に失敗した場合は，[Payloads] データの該当行に INVALID と記述する．

2.5 結果ファイル (*.out)

表 10: CCM モード結果ファイル

タグ	内容
[Algorithm Name]	暗号名
[Function Name]	試験対象機能名
[Results]	試験結果

注

- 試験合格の場合，[Results] に OK と表示される．
- 試験不合格の場合，[Results] に何らかの形式で NG と表示される．また，[Results] には，レスポンスファイル内の不合格となったデータが記述されているタグ名と，そのタグ内の何番目 (No.，#等の記号で番号を表す) のデータが不合格となったかが表示される．不合格となったデータが記述されているタグ名は，前記のレスポンスファイル仕様に【出力】と記述したタグである．ただし,【出力】と記述したタグが 1 つしかない場合，タグ名は省略することがある．